“The Right to Be Let Alone”

Privacy ... is a fundamental human right and plays an important role in human dignity, put by U.S. Supreme Court Justice Louis Brandeis as “the right to be let alone ... the right most valued by civilized men.”
—UCLA Statement on Privacy (in draft)

How does a higher education institution decide whether to allow the monitoring of all outbound e-mails for telltale signs of confidential information being leaked? Or to allow the use of its students, faculty, and staff as unknowing subjects for research in which all their search queries to Google are captured? Or to allow the monitoring of all network traffic for infringing uses of copyrighted materials? Is it ever possible to be “let alone” when working with confidential information?

These questions are hard to answer in the same way that questions about individual privacy versus the security of the nation are hard to answer: differing values, changing technology, and evolving law and culture frame a vortex within which higher education institutions, like the nation, must continuously balance between (often competing) values and obligations. And since new technology is frequently the driver that causes a need for reevaluation, it is into the laps of chief information officers that such questions usually fall, with demands to use the master cyberkeys in their possession to give access to information. CIOs themselves are often directly accountable for security. Yet these questions of balance are institutional questions that speak to the core of the institution’s mission—thus necessitating an institutional conversation.

Privacy versus Privacy versus Privacy

Three interrelated concepts are relevant in this discourse:

- **Privacy as a civil liberty**: safeguarding the privacy of individuals, which speaks to Brandeis’s “right to be let alone”—freedom from surveillance, from Big Brother, and from the monitoring of behavior
- **Data protection**: safeguarding the confidentiality of information about individuals
- **Security**: safeguarding the infrastructure—the systems and networks—that hold and transport electronic data and communications

Confusion arises because the word privacy is commonly used to denote all three concepts. For example, many state breach-notification laws refer to security breaches—that is, infrastructural breaches that permit unauthorized access to confidential data—whereas many privacy officers refer to such breaches as privacy breaches to indicate that confidential information about people has been breached.

The traditional debate has been about how much security is appropriate: whereas security techniques and technologies that are used to protect information and infrastructure also protect people’s privacy (e.g., encryption to prevent eavesdropping), they can be used to invade that privacy as well (e.g., security cameras in washrooms). In fact, security and data protection are only two of a class of operational imperatives that are important to the higher education institution but that also have implications for individual privacy:

- **E-discovery requirements**, which can force the potentially indefinite retention of e-mails, documents, and other relevant materials when litigation is anticipated
- **Public records laws**, which make most e-mails, documents, voicemails, and the like available to members of the public to ensure transparency and accountability of institutions that use taxpayer money
- **Web analytics tools**, which any webmaster is expected to use to understand how effective a website is: how visitors navigated pages, whether they found the information sought, whether important messages were seen

Each of these operational imperatives has a legal or financial consequence, often of large magnitude, for failure to do due diligence. A security breach of Social Security numbers can have legal, financial, and reputational consequences; failure to retain the right documents during e-discovery can result in fines. For this reason, the private sector rarely extends individual privacy rights to employees beyond what the law requires; doing otherwise can lead to additional legal risk. But in higher education, privacy—the civil liberty—underpins academic freedom, which in turn underpins the institution. Of course, so too does an environment of openness and innovation. The balancing tests are much more difficult in higher education.

Privacy and Higher Education

The draft UCLA Statement on Privacy notes: “Privacy is an underpinning of academic freedom, upon which the mission of the University is dependent. Academic freedom is most vibrant where individuals have autonomy: where their inquiry is free because it is given adequate space for experimentation
and their ability to speak and participate in discourse within the academy is possible without intimidation.” Consider a scenario in which all queries made by students, faculty, and staff from a campus to, say, Google will be captured for search engine research. Of course, this data is de-identified so that no query can be linked back to the individual who made it (though it should be noted that computer scientists are “breaking” de-identification techniques all the time). What would the reaction be if these people knew that every query they made was being intercepted and stored? Doubtless there would be a change in behavior—which is precisely why the research subjects couldn’t be told in advance that they were part of the research.

Now shift this to the administrative context. If the IT department's firewall logs every website being visited by any student, faculty, or staff, is this any different? What if those logs are kept indefinitely in case an incident arises in the future and there is a need to know who was doing what at a specific time, whether for human resources purposes, litigation, or a security incident? Would people behave differently? On the one hand, a behavioral shift may be desirable. On the other hand, this change in behavior can put a chill on academic freedom.

Even after compliance with law and regulation, there exists substantial room for choice in the approach that a higher education institution takes to individual privacy. (Academic medical centers, which exist in a highly regulated environment, have narrower room for choice.) Governance and policy are the standard means for having the institutional conversations needed to make institutional choices: the governance structure brings together the right voices for discussion and deliberation; the policy articulates the expectations about individual privacy for the campus community. Together, they form a process for considering the changing laws and needs and the changing interpretations of privacy.

A Governance Policy Model

Let's revisit the search engine research scenario. Does the privacy right of the campus community trump a legitimate research project, especially considering that research is a fundamental mission of many institutions? What if the researcher could instead simply buy this data directly from one or more search companies? And what about the privacy right of the institution? For example, what if the researcher found that there seemed to be a surprising number of people on campus searching for how to build a bomb? The data is de-identified, but is attention from intelligence agencies in the best interests of the institution?

An institution can take advantage of its existing IT governance structure to talk about privacy, but UCLA has discovered that the conversations can be much richer if held by a group that has the time and space to focus deeply on privacy principles rather than operations. UCLA thus formed the Advisory Board on Privacy and Data Protection (http://privacyboard.ucla.edu/), reporting to the Executive Vice Chancellor and Provost, to fulfill this role. Bringing together students, faculty experts from diverse backgrounds, and senior administrators with related operational roles, the Privacy Board has discussed issues such as the techniques to use for combating illegal file-sharing, the appropriate use of social networking technologies from an institutional viewpoint (rather than from a student viewpoint, though that too has come up), proposed revisions to university policies, IT security techniques, and breaches and legal compliance. The Privacy Board takes a principled view in converging the threads of discourse with the university’s primary missions and due-diligence obligations.

Out of its many conversations, the Privacy Board has begun developing a privacy statement. The statement is intended to express the institutional context for making operational decisions when privacy implications are present. Neither a policy nor a procedure, it begins simply with the statement that privacy is important to UCLA and explains why, then identifies other institutional obligations and values with which privacy must be balanced. More concretely, it articulates a set of fair information practices that guide the development of systems: transparency; privacy-friendly design; accountability and fairness; and sustainability and operational necessity. These practices are based on the Organisation for Economic Co-operation and Development (OECD) Fair Information Principles that underlie the architecture of privacy legislation such as HIPAA and FERPA. The statement also describes how UCLA interprets certain areas of the University of California systemwide policy, and it will include a few scenarios to directly tie concepts in the statement with real-life situations.

The ultimate goal is for the Privacy Board to consider any new privacy issue within the context of the university’s policies and the law and in light of the principles, guidance, and scenarios of its privacy statement. When a privacy issue is straightforward or operational, a single campus official may appropriately adjudicate between, and be the lightning rod for, the inevitable differences of opinion. But a stronger position is achieved when the voices of many different perspectives converge. In new and complex cases, an institutional governance policy model can serve as the lightning rod for the difficult decisions to be made about the right to privacy—that is, the “right to be let alone.”

Notes

2. Ibid.

Kent Wada (kent@ucla.edu) is Director, Strategic IT and Privacy Policy, at UCLA. He helps shape institutional policy in domains of national concern such as privacy, security, and copyright in light of evolving technologies.

© 2010 Kent Wada. The text of this article is licensed under the Creative Commons Attribution-Noncommercial-Share Alike 3.0 Unported License (http://creativecommons.org/licenses/by-nc-sa/3.0/).